



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,385	01/06/2004	Hashem M. Ebrahimi	1565.066US1	6809
21186 7590 05/28/2008 SCHWEGMAN, LUNDBERG & WOESSNER, P.A. P.O. BOX 2938 MINNEAPOLIS, MN 55402				
EXAMINER				
LE, CANH				
ART UNIT		PAPER NUMBER		
2139				
MAIL DATE		DELIVERY MODE		
05/28/2008		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

**Office Action Summary****Application No.**

10/752,385

**Applicant(s)**

EBRAHIMI ET AL.

**Examiner**

CANH LE

**Art Unit**

2139

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 10 March 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,2,6,8,10 and 12-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,6,8,10 and 12-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/S508)  
Paper No(s)/Mail Date 03/10/2008
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

This Office Action is in response to the communication filed on 03/10/2008.

Claims 3-5, 7, 9, 11, and 22-30 have been cancelled.

Claims 1, 8, 10, and 16 have been amended.

Claims 1, 2, 6, 8, 10 and 12-21 have been examined and are pending.

### ***Response to Arguments***

Applicant's arguments regarding the objection of claim 10, filed 03/10/2008, see page 6, filed 03/10/2008, have been fully considered and are persuasive. The objection of claim 10 has been withdrawn.

Applicant's arguments regarding the 112, 1<sup>st</sup> rejection of claims 1, 2, 6, 8, 10-15, and 16-21, see page 6, filed 03/10/2008, have been fully considered and are persuasive. The rejection of claims 1, 2, 6, 8, 10-15, and 16-21 has been withdrawn.

Applicant's arguments filed 03/10/2008 have been fully considered but they are not persuasive.

**With regard to claim 1**, the Applicant argues that Subramaniam does not address the following limitations:

- *“when a resource was reference outside the secure network (firewall) by the authentication client.”*
- *“external client attempts to reference a resource outside of the secure environment.”*

**The Examiner** respectfully disagrees with the following reasons:

Subramaniam discloses a method to manage secure communications, comprising:

(a) establishing a secure session on a secure site with an external client that communicates from an insecure site [*Col. 3 lines 35-50; Col. 3, line 66 to Col. 4 line 17*];

(b) detecting access attempts during the session directed to insecure transactions, the insecure transactions identified as links to a site [*Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102. The target server 104 check user permission against access control list associated with the data*”; *fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; “The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ....which contain URLs specifying “http://” rather than “https://” in reference to data stored on the target server 104 are examples of non-secure data 130*”; *Col. 10, lines 10-19*]; and

(c) transparently managing the access attempts by pre-acquiring content from the secure site by accessing the links on behalf of the client to pre-acquire the content and by scanning the content before determining whether the content should be made available to the external client during the secure session [*Col. 6, lines 40-60; The target server 104 checks user permission against access control list associated with the data, or take other steps to make sure the requesting user is entitled to access the request data before providing data*”; *fig. 1, Border*

*server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; “The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ....which contain URLs specifying “http://” rather than “https://” in reference to data stored on the target server 104 are examples of non-secure data 130”; Col. 10, lines 10-19]. Further more, figure 1 shows that “The target server 104 checks user permission against access control list associated with data.” This process could be interpreted as “managing the access attempts by pre-acquiring the content the content on behalf of the client and inspecting it within the secure site.”*

Subramaniam does not teach wherein the border server is external from the secure site.

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made **to move the border server to a site external from the secure location (emphasis added)** , since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device [See MPEP 2144.04; see also *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)] and enhanced security by scanning a content outside of security network 100.

In addition, the Applicant argues that the “*applicant provided a solution that is defined in the claims, namely pre-acquiring the content on behalf of the client and inspecting it within the secure site.*” However, the term “*inspecting it within the secure site,*” is not mentioned in the claim language.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., namely *pre-acquiring* the content on behalf of the client and **inspecting it within the secure site.**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

**With regard to claim 17**, the applicant argues that “internal resources that are internally addressed with the firewall are not address using *secure protocols*.”

The Examiner respectfully disagrees as the following reasons:  
Subramaniam discloses the secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session [*Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPS)*]. HTTPS is a secure protocol.

**With regard to independent claims 8 and 16** (See the same arguments above).

The fact that Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative should not be construed as indicating Examiner's agreement therewith.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1-2, 6, 8, 13, and 16-17** are rejected under 35 U.S.C. 103(a) as being anticipated by **Subramaniam et al.** (US Patent: 6,081,900).

**As per claim 1:**

Subramaniam discloses a method to manage secure communications, comprising:

- (a) establishing a secure session on a secure site with an external client that communicates from an insecure site [**Col. 3 lines 35-50; Col. 3, line 66 to Col. 4 line 17**];
- (b) detecting access attempts during the session directed to insecure transactions, the insecure transactions identified as links to a site [**Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102. The target server 104 check user permission against access control list associated with the data**”; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; “The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs,

**or other references which, if presented by the external client 112 to the secure network 100, ....which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19]; and**

(c) transparently managing the access attempts by pre-acquiring content from the secure site by accessing the links on behalf of the client to pre-acquire the content and by scanning the content before determining whether the content should be made available to the external client during the secure session [Col. 6, lines 40-60; **The target server 104 check user permission against access control list associated with the data, or take other steps to make sure the requesting user is entitled to access the request data before providing data"; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ....which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19].**

Subramaniam does not teach wherein the border server is external from the secure site.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server



because it would not have modified the operation of the device [See MPEP 2144.04; see also *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].

**As per claim 2:**

Subramaniam further discloses the method of claim 1 wherein the detecting further includes translating non-secure links into secure links for the insecure transactions before presenting results of the access attempts to the external client [Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPS)].

**As per claim 6:**

Subramaniam discloses the method of claim 1 wherein managing further includes at least one or more of:

issuing alerts [Col. 11, lines 61-67], notifications [Col. 8, lines 40-57], or advisories to a monitoring entity or log.

**As per claim 8:**

Subramaniam discloses a method to manage secure communications, comprising:

(a) detecting insecure transactions occurring during a secure session, wherein the insecure transactions result from actions requested by an external client participating in the secure session [Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102];

(b) inspecting the insecure transactions in advance of satisfying the actions requested by pre-acquiring content associated with the insecure transactions before making available to the

external client , and wherein the insecure transactions are associated with links to an site, and wherein content are pre-acquired from the site via the links and scanned on behalf of the client [Col. 6, lines 46-60; A target server check user permissions against access control lists; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; “The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ....which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130”; Col. 10, lines 10-19]; and

making a determination in response to the inspection for at least one of the following: permitting the insecure transactions to proceed unmodified by performing the actions requested for the external client, permitting the insecure transactions to proceed in a modified fashion [Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPS)], and denying the insecure transactions by denying the actions requested.

Subramaniam does not teach wherein the border server is external from the secure site.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device [See MPEP 2144.04; see also *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].

**As per claim 13:**

Subramaniam further discloses the method of claim 8 wherein the making a determination further includes permitting the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure session [Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPS)].

**As per claim 16:**

This claim has limitations that are similar to those of claims 1 and 8, thus it is rejected with the same rationale applied against claims 1 and 8 above.

**As per claim 17:**

Subramaniam further discloses the secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session [Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPS)].

Claims 10, 12, 14-15, and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Subramaniam et al. (US Patent: 6,081,900) in view of "Netscape Proxy Server Administrator's Guide Version 3.5 for Unix", 1997, as provided by applicant herein after Netscape\_unix\_v3.5.

**As per claim 10:**

Subramaniam further discloses a method permitting the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) [Col. 3, lines 66-67; Col. 4, lines 1-8; **Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPS)**].

Subramaniam does not disclose to suppress the security warning messages. Netscape\_unix\_v3.5 discloses to suppress the security warning messages [Chapter 10, pages 1-3; **A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text**].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape\_unix\_v3.5 because it would improve techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated [**the background of this application**].

**As per claim 12:**

Subramaniam discloses the method as described in claim 8.

Subramaniam does not disclose a method permitting insecure transactions to proceed unmodified.

The background of the invention discloses a method permitting insecure transactions to proceed unmodified [Col. 2, lines 36-41].

Subramaniam and the background of the invention do not disclose permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site.

Netscape\_unix\_v3.5 discloses permitting normally occurring security warnings to be presented to external the client before satisfying the external client access attempt to reference the external site [Chapter 10, pages 1-3; Chapter 13, page 1; **A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages**].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify Subramaniam and the method of the background of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application]**.

**As per claim 14:**

Subramaniam discloses the method as described in claim 8.

Subramaniam does not disclose a method as described in claim 14.

Netscape\_unix\_v3.5 discloses the method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of the denial [Chapter 13, page 1; **A proxy**

**will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

**As per claim 15:**

Subramaniam discloses the method as described in claim 8.

Subramaniam does not disclose a method as described in claim 15.

Netscape\_unix\_v3.5 further discloses the method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt **[Chapter 13, pages 1-7].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

**As per claim 18:**

Subramaniam further discloses the secure communications management system of claim 16 wherein the proxy selectively modifies a number of the insecure communications [Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8].

Subramaniam does not disclose to suppress normally occurring security warning messages that the secure communications manager issues.

Netscape\_unix\_v3.5 discloses to suppress normally occurring security warning messages that the secure communications manager issues [Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated [the background of this application].

**As per claim 19:**

The background of the invention discloses the secure communications management system of claim 16 wherein the proxy selectively leaves a number of the insecure communications unchanged [Col. 2, lines 36-41].

The background of the invention does not disclose to issue security warning messages to the external client.

Netscape\_unix\_v3.5 discloses a proxy sending security warning messages to the external client [Chapter 10, pages 1-3; Chapter 13, page 1; **A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages**].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of the background of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated [**the background of this application**].

**As per claim 20:**

Subramaniam discloses the secure communication system as claimed in claim 16.

Subramaniam does not disclose a proxy which selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log.

Netscape\_unix\_v3.5 discloses a proxy which selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log [Chapter 13, page 1; **A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt; Proxy error log messages include Catastrophe error, Failure, information log entry, warning flags, and security warning**].



Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application]**.

**As per claim 21:**

Subramaniam discloses the secure communication system as claimed in claim 16.

Subramaniam does not disclose a proxy selectively sending custom warning messages or explanations to the external client regarding a number of the insecure communications.

Netscape\_unix\_v3.5 discloses a proxy which selectively issues custom warning messages or explanations to the external client regarding a number of the insecure communications **[Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape\_unix\_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application]**.

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kincaid Kristine can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)? If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Lc/

Examiner, Art Unit 2139

May 18, 2008

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139